IN THE CLAIMS

Please amend the claims as follows:

1.-4. (Canceled)

5. (Withdrawn) A data processing method for verifying legitimacy of identification data assigned to recording media for identifying the recording media, comprising:

a step of using public key data of the management side of said identification data to verify the legitimacy of said identification data.

6. (Withdrawn) A data processing method as set forth in claim 5, wherein said step has

a first step of generating the first data from said signature data included in said identification data by using said public key data and

a second step of comparing the second data included in said identification data and said first data generated at said first step and verifying the legitimacy of said identification data based on the result of the comparison.

7. (Withdrawn) A program executed by a data processing apparatus for verifying legitimacy of identification data for identifying recording media assigned to the recording media, comprising

a routine for using public key data of a management side of said identification data to verify the legitimacy of said identification data.

8. (Withdrawn) A data processing apparatus for verifying the legitimacy of identification data for identifying recording media assigned to said recording media, comprising:

a means for using public key data of a management side of said identification data to verify the legitimacy of said identification data.

9. (Withdrawn) A data processing method for generating identification data for identifying recording media, comprising:

a first step of using secret key data and data S of a management side of said identification data to generate a plurality of different signature data able to decode said data S based on public key data of the management side and

a second step of generating identification data including signature data and said data S for each of said plurality of signature data generated at said first step and assigning said plurality of identification data to the different plurality of recording media.

10. (Withdrawn) A data processing as set forth in claim 9, further having a third step of writing the encryption data encrypted by using said data S as the encryption key and said identification data into said recording media.

11. (Withdrawn) A program executed by a data processing apparatus for generating identification data for identifying recording media, comprising:

a first routine for using secret key data and data S of a management side of said identification data to generate a plurality of different signature data able to decode the data S based on said public key data of the management side and

a second routine for generating identification data including signature data and said data S for each of said plurality of signature data generated by said first routine and assigning said plurality of identification data to the different plurality of recording media respectively.

12. (Withdrawn) A data processing apparatus for generating identification data for identifying recording media, comprising:

a first means for using secret key data and data S of a management side of said identification data to generate a plurality of different signature data able to decode data S based on said public key data of the management side and

a second means for generating identification data including signature data and the data S for each of said plurality of signature data generated by said first means and assigning said plurality of identification data to the different plurality of recording media respectively.

13. (Withdrawn) A data processing method for verifying the legitimacy of identification data for identifying recording media assigned to recording media, comprising:

a first step of using public key data of a management side of said identification data to generate first data from signature data in said identification data and comparing the first data and second data in said identification data to verify the legitimacy of said identification data and

a second step of decoding encryption data read out from said recording media by using said second data in said identification data when it is verified at said first step that said identification data is legitimate.

14. (Withdrawn) A program executed by a data processing apparatus for verifying the legitimacy of identification data for identifying recording media assigned to the recording media, comprising:

a first routine for using public key data of a management side of said identification data to generate first data from signature data in said identification data and comparing the first data and second data in said identification data to verify the legitimacy of said identification data and

a second routine for decoding encryption data read out from said recording media by using said second data in said identification data when it is verified by said first routine that said identification data is legitimate.

15. (Withdrawn) A data processing apparatus for verifying the legitimacy of the identification data for identifying the related recording media assigned to the recording media, comprising:

a first means for using public key data of a management side of said identification data to generate first data from signature data in said identification data and comparing the first data and second data in said identification data to verify the legitimacy of said identification data and

a second means for using said second data in said identification data to decode encryption data read out from said recording media when it is verified by said first means that said identification data is legitimate.

16. (Withdrawn) A data processing method for generating identification data ID(w) individually assigned to W number of recording media STM(w) where the opened data M is a product of two prime numbers, T is a product of W ($W \geq 2$) number of different prime

numbers p(w), w is an integer of $1 \leqq w \leqq W$, and K is a generator of a cyclic group Z*M, comprising:

a first step of calculating (KT/p(w) modM) and

a second step of assigning the identification data ID(w) including (KT/p(w) modM) calculated at said first step to the recording media STM(w).

17. (Withdrawn) A data processing method as set forth in claim 16, further having a third step of writing the encryption data encrypted by using (KT modM) as the encryption key and said identification data ID(w) into said recording media STM(w).

18. (Withdrawn) A program executed by a data processing apparatus for generating identification data ID(w) individually assigned to W number of recording media STM(w) where opened data M is a product of two prime numbers, T is a product of W ($W \geq 2$) number of different prime numbers p(w), w is an integer of $1 \leqq w \leqq W$, and K is a generator of a cyclic group Z*M, comprising:

a first routine for calculating (KT/p(w) modM) and

a second routine for assigning identification data ID(w) including (KT/p(w) modM) calculated by said first routine to the recording media STM(w).

19. (Withdrawn) A data processing apparatus for generating identification data ID(w) assigned to W number of recording media STM(w) where opened data M is a product of two prime numbers, T is a product of W ($W \geq 2$) number of different prime numbers p(w), w is an integer of $1 \leqq w \leqq W$, and K is a generator of a cyclic group Z*M, comprising:

a first means for calculating (KT/p(w) modM) and

a second means for assigning identification data ID(w) including (KT/p(w) modM) calculated by said first means to the recording media STM(w).

20. (Withdrawn) A data processing method for verifying a legitimacy of identification data for identifying recording media assigned to the recording media, comprising:

a first step of verifying whether or not data p included in said identification data is a prime number;

a second step of using data IDKey and said data p included in said identification data and opened data M to calculate (IDKeyp modM) when it is verified at said first step that said data p is a prime number; and

a third step of using a decoding key obtained based on (IDKeyp modM) calculated at said second step to decode encryption data recorded at said recording media.

21. (Withdrawn) A program executed by a data processing apparatus for verifying a legitimacy of identification data for identifying recording media assigned to the recording media, comprising:

a first routine for verifying whether or not data p included in said identification data is a prime number;

a second routine for using data IDKey and said data p included in said identification data and opened data M to calculate (IDKeyp modM) when it is verified by said first routine that said data p is a prime number; and

a third routine for using a decoding key obtained based on (IDKeyp modM) calculated by said second routine to decode the encryption data recorded in said recording media.

22. (Withdrawn) A processing apparatus for verifying a legitimacy of identification data for identifying recording media assigned to recording media, comprising:

a first means for verifying whether or not the data p included in said identification data is a prime number;

a second means for using the data IDKey and said data p included in said identification data and opened data M to calculate (IDKeyp modM) when it is verified by said first means that said data p is a prime number; and

a third means for using a decoding key obtained based on (IDKeyp modM) calculated by said second means to decode the encryption data recorded in said recording media.

23. (Withdrawn) A data processing method for generating identification data ID(w) assigned to each of W number of recording media STM(w) when data which is the product of the prime numbers q1 and q2 and is opened is M, w is an integer of $1 \leqq w \leqq W$, W ($W \geq 2$) number of different data are e(w), e(w) is a generator of a cyclic group Z*M, e(w) and λ(M) are primes with respect to each other, and λ(M) is the least common multiple of (q1-1) and (q2-1), comprising:

a first step of using the data S of the generator of a cyclic group Z*M to calculate (Sd(w) modM), the data d(w) of the reciprocal of e(w) when λ(M) is normal, and said data M and

a second step of assigning identification data ID(w) including the (Sd(w) modM) calculated at said first step to the recording media STM(w).

24. (Withdrawn) A data processing method as set forth in claim 23, further having a third step of writing the encryption data encrypted by using said data S as the encryption key and said identification data ID(w) into said recording media STM(w).

25. (Withdrawn) A program executed by a data processing apparatus for generating identification data ID(w) assigned to each of W number of recording media STM(w) when data which is a product of prime numbers q1 and q2 and is opened is M, w is an integer of $1 \leqq w \leqq W$, W ($W \geq 2$) number of different data are e(w), e(w) is a generator of a cyclic group Z*M, e(w) and $\lambda(M)$ are primes with respect to each other, and $\lambda(M)$ is the least common multiple of (q1-1) and (q2-1), comprising:

a first routine for using the data S of the generator of a cyclic group Z*M, the data d(w) of a reciprocal of e(w) when $\lambda(M)$ is normal, and said data M to calculate (Sd(w) modM) and

a second routine for assigning identification data ID(w) including (Sd(w) modM) calculated by said first routine to the recording media STM(w).

26. (Withdrawn) A data processing apparatus for generating identification data ID(w) assigned to each of W number of recording media STM(w) when data which is a product of prime numbers q1 and q2 and opened is M, w is an integer of $1 \leqq w \leqq W$, W ($W \geq 2$) number of different data are e(w), e(w) is a generator of a cyclic group Z*M, e(w) and $\lambda(M)$ are primes with respect to each other, and $\lambda(M)$ is the least common multiple of (q1-1) and (q2-1), comprising:

a first means for using the data S of the generator of a cyclic group Z*M, the data d(w) of a reciprocal of e(w) when $\lambda(M)$ is normal, and said data M to calculate (Sd(w) modM) and

a second means for assigning identification data ID(w) including (Sd(w) modM) calculated by said first means to the recording media STM(w).

27. (Withdrawn) A data processing method for verifying a legitimacy of identification data for identifying recording media assigned to the recording media, comprising:

a first step of using data e and data I included in said identification data and opened data M to calculate (Ie modM) and

a second step of using (Ie modM) calculated at said first step as the decoding key to decode the encryption data recorded in said recording media.

28. (Withdrawn) A program executed by a data processing apparatus for verifying the legitimacy of identification data for identifying recording media assigned to the recording media, comprising:

a first routine for using data e and data I included in said identification data and opened data M to calculate (Ie modM) and

a second routine for using (Ie modM) calculated by said first routine as the decoding key to decode the encryption data recorded in said recording media.

29. (Withdrawn) A data processing apparatus for verifying a legitimacy of identification data for identifying recording media assigned to the recording media, comprising:

a first means for using data e and data I included in said identification data and opened data M to calculate (Ie modM) and

a second means for using (Ie modM) calculated by said first means as the decoding key to decode encryption data recorded in said recording media.

30. (Withdrawn) A recording medium for recording data, recording identification data generated by using secret key data of a management side of said recording medium, verified in legitimacy based on the public key data of said management side, and identifying the recording medium.

31. (Withdrawn) A recording medium for recording data, recording identification data including signature data used for generating first data by using public key data of a management side of said recording medium and said second data used for verifying a legitimacy of the identification data by comparing the same with said first data and identifying said recording medium.

32. (Withdrawn) A recording medium for recording encryption data, recording identification data including

data p of a prime number and

data IDKey used for calculating (IDKeyp modM) of content key data used for decoding said encryption data together with said data p and the opened data M and

identifying said recording medium.

33. (Withdrawn) A recording medium for recording encryption data, recording identification data including data e used for calculating (Ie modM) of content key data used for decoding said encryption data together with opened data M and data I and identifying said recording medium.

34.-36. (Canceled)

37. (Currently Amended) A method of a media verification system for identifying recording media, comprising:

generating a plurality of different signature data elements from a secret key data element and a message data element using a data processing device of the media verification system;

generating a plurality of different identification data elements using the data processing device, each of the plurality of different identification data elements including a generated signature data element and [[a]] the message data element used in the generating of the generated signature data elements, and storing the plurality of different identification data elements in an electronic memory of the media verification system;

assigning one of the plurality of generated identification data elements to each of a plurality of different recording media;

recording one of the plurality of generated identification data elements to an assigned recording media using a media writing device of the media verification system;

generating a verification data element from the generated signature data element of the identification data element recorded on the assigned recording media using a public key;

comparing the verification data element to the message data element of the identification data element recorded on the assigned recording media using the data processing device to determine whether the verification data element and the message data element of the identification data element recorded on the assigned recording media are the same, and verifying the identification data element [[if]] based upon a determination that the

verification data element is the same as the message data element of the identification data recorded on the assigned recording media; and

writing an encrypted content to the assigned recording media using a media recording device [[if]] based upon a determination that the assigned recording media is verified in the comparing, wherein the media recording device is configured to inhibit writing the encrypted content to a recording media having an unverified identification data element or no identification data element recorded thereon.

38. (Currently Amended) The method according to Claim 37, further comprising:

generating an identification revocation list, wherein the identification revocation list includes an identification data element corresponding to an unauthorized recording media; and

recording the identification revocation list to the assigned recording media using the media writing device, wherein

the media recording device is further configured to inhibit writing the encrypted content to the assigned recording media [[if]] based upon a determination that the identification data element recorded on the assigned recording media is included in the identification revocation list.

39. (Currently Amended) A computer readable medium including computer executable instructions, wherein the instructions, when executed by a data processing device, cause the data processing device to perform a method for generating identification data for identifying recording media, the method comprising:

generating a plurality of different signature data elements from a secret key data element and a message data element using a data processing device;

generating a plurality of different identification data elements using the data processing device, each of the plurality of different identification data elements including a generated signature data element and [[a]] the message data used in the generating of the generated signature data elements, and storing the plurality of different identification data elements in an electronic memory;

assigning one of the plurality of generated identification data elements to each of a plurality of different recording media;

recording one of the plurality of generated identification data elements to an assigned recording media using a media writing device;

generating a verification data element from the generated signature data element of the identification data element recorded on the assigned recording media using a public key;

comparing the verification data element to the message data element of the identification data element recorded on the assigned recording media using the data processing device to determine whether the verification data element and the message data element of the identification data element recorded on the assigned recording media are the same, and verifying the identification data element [[if]] based upon a determination that the verification data element is the same as the message data element of the identification data element recorded on the assigned recording media; and

writing an encrypted content to the assigned recording media using a media recording device [[if]] based upon a determination that the assigned recording media is verified in the comparing, wherein the media recording device is configured to inhibit writing the encrypted content to a recording media having an unverified identification data element or no identification data element recorded thereon.

40. (Currently Amended) The computer readable medium according to Claim 39, the method further comprising:

generating an identification revocation list, wherein the identification revocation list includes an identification data element corresponding to an unauthorized recording media; and

recording the identification revocation list to the assigned recording media using the media writing device, wherein

the media recording device is further configured to inhibit writing the encrypted content to the assigned recording media [[if]] based upon a determination that the identification data element recorded on the assigned recording media is included in the identification revocation list.

41. (Currently Amended) A media verification system for identifying recording media, comprising:

a data processing device configured to

generate a plurality of different signature data elements from a secret key data element and a message data element,

generate a plurality of different identification data elements, wherein each of the plurality of different identification data elements includes a generated signature data element and [[a]] the message data element used in generating of the generated signature data elements,

store the plurality of different identification data elements in an electronic memory, and

assign one of the plurality of generated identification data elements to each of a plurality of different recording media;

a media writing device configured to record one of the plurality of generated identification data elements to an assigned recording media;

a data processing device configured to generate a verification data element from the generated signature data element of the identification data element recorded on the assigned recording media using a public key;

a comparison device configured to compare the verification data element to the message data element of the identification data element recorded on the assigned recording media and verify the identification data element [[if]] based upon a determination that the verification data element is the same as the message data element of the identification data element recorded on the assigned recording media; and

a media recording device configured to record an encrypted content to the assigned recording media [[if]] based upon a determination that the assigned recording media is verified by the comparison device, and the media recording device is further configured to inhibit writing the encrypted content to a recording media having an unverified identification data element or no identification data element recorded thereon.

42. (Currently Amended) The media verification system according to Claim 41, further comprising:

a data processing device configured to generate an identification revocation list, wherein the identification revocation list includes an identification data element corresponding to an unauthorized recording media; and

a media writing device configured to record the identification revocation list to the assigned recording media, wherein

the media recording device is further configured to inhibit writing the encrypted content to the assigned recording media [[if]] based upon a determination that the

identification data element recorded on the assigned recording media is included in the identification revocation list.